All the optimal stabilizer codes of distance 3

Sixia Yu, Ying Dong, Qing Chen, and C.H. Oh

***Abstract*— Optimal quantum stabilizer codes of distance 3 are explicitly constructed for all lengths except for the following four families of lengths $8f_m-\{1,2\}$ and $f_{m+2}-\{2,3\}$ with $f_m=\frac{4^m-1}{3}$ and $m\geq 2$ being integer, for which our codes are of the best parameters known and are only one logical qubit less than the quantum Hamming bound. The optimality of our codes is ensured by saturating either the quantum Hamming bound or a stronger bound for three families of lengths $8f_m+\{1,2\}$ and $f_{m+2}-1$ with $m\geq 1$ derived from the linear programming bound. For the lengths less than 128 three previously unknown codes $[[36,29,3]]$, $[[37,30,3]]$ and $[[81,73,3]]$ have been found.**

***Index Terms*— quantum error correction, 1-error correcting stabilizer codes, quantum Hamming bound, linear programming bound, optimal codes**

I. Introduction

Quantum error-correcting codes [2], [9], [13], [15] provide us an active way of protecting our precious quantum data from quantum noises and play essential roles in various quantum informational processes. Simply speaking, a QECC is just a subspace that corrects certain type of errors. When the subspace is specified by the joint +1 eigenspace of a group of commuting multilocal Pauli operators, i.e., direct products of local Pauli operators, the codes are called as stabilizer codes [3], [4], [5]. We consider only binary codes here. As usual we shall denote by $[[n,k,d]]$ a stabilizer code of length n and distance d, i.e., correcting up to $\lfloor\frac{d-1}{2}\rfloor$-qubit errors, that encodes k logical qubits.

One fundamental task is to construct optimal codes, e.g., codes with largest possible k with fixed n and d. In the case of $d=2$ all optimal stabilizer codes are known. In the simplest nontrivial case $d=3$, despite many efforts to construct optimal stabilizer codes, a systematic construction for all lengths has not been achieved yet. Known results include Gottesman's optimal codes family [6] of lengths 2^m with $m\geq 3$ which has been generalized for even lengths [10] by using Steane's enlargement construction [16] with some codes being optimal and some are suboptimal, i.e., one logical qubit less than the quantum Hamming bound.

A code of distance d is *degenerate* if there are harmless undetectable errors acting on less than d qubits, i.e., errors can not be detected but do not affect the encoded quantum data. If all errors acting on less than d qubits can be detected the codes are *non-degenerate* or *pure*. For a pure code of distance 3 all errors happened on up to 2 qubits can be detected. The quantum Hamming bound, e.g.,

$$n-k\geq s_H=\lceil\log_2(3n+1)\rceil \tag{1}$$

Sixia Yu, Ying Dong, Qing Chen are with the Department of Modern Physics, University of Science and technology of China, China

Sixia Yu and Qing Chen, and C.H. Oh are with Physics department, National University of Singapore, 2 Science drive 3, Singapore

The financial supports from NSF Grant No. 10675107, No. 10705025, and A*STAR grant R-144-000-189-305 are acknowledged.

TABLE I

A summary of the existence of optimal stabilizer codes $[[n,k,3]]$ of all lengths. All these codes saturate the quantum Hamming bound except for 7 families of lengths with 3 of them (labeled by l) being nevertheless optimal and 4 of them (labeled by u) having the best parameters known.

n	$n-k$	s_H
5	4	4
${}^{\beta}6,8$	5	5
$7,9,10$	6	5
$11\leq n\leq 17,21$	6	6
$18,19,\ {}^{l}20$	7	6
$22\leq n\leq 35,\ {}^{\alpha}36,\ {}^{\alpha}37,40$	7	7
${}^{u}38,\ {}^{u}39,\ {}^{l}41,\ {}^{l}42$	8	7
$43\leq n\leq\ {}^{\alpha}81,85$	8	8
${}^{u}82,\ {}^{u}83,\ {}^{l}84$	9	8
$86\leq n\leq 128$	9	9
$f_{m+1}+1\leq n\leq 8f_m-3\ (m\geq 2)$	$2m+3$	$2m+3$
${}^{p}(8f_m)\ (m\geq 1)$	$2m+3$	$2m+3$
$8f_m-\{{}^{u}1,\ {}^{u}2\}\ (m\geq 2)$	$2m+4$	$2m+3$
$8f_m+\{{}^{l}1,\ {}^{l}2\}\ (m\geq 1)$	$2m+4$	$2m+3$
$8f_m+3\leq n\leq f_{m+2}-4\ (m\geq 2)$	$2m+4$	$2m+4$
${}^{p}f_{m+2}\ (m\geq 0)$	$2m+4$	$2m+4$
$f_{m+2}-\{{}^{u}2,\ {}^{u}3\}\ (m\geq 2)$	$2m+5$	$2m+4$
${}^{l}(f_{m+2}-1)\ (m\geq 1)$	$2m+5$	$2m+4$

for a stabilizer code $[[n,k,3]]$, is introduced initially for the non-degenerate codes, has been proved to be valid for degenerate codes of distance 3 and 5 [5] and of a large enough length [1] via linear programming (LP) bound [4], [11].

The most comprehensive list of stabilizer codes of distance 3 up to 128 qubits is presented in the public code table maintained by Grassl [8] and the parameters of the optimal codes are summarized in the upper half of Table I, where the optimal codes of length labeled by l do not saturate the quantum Hamming bound and the optimal code of length $n=6$ (labeled by β) is degenerate. Those optimal codes of three lengths labeled with α are previously unknown and will be constructed here.

In this paper we shall construct explicitly the optimal stabilizer codes of all lengths and a summary is given in the lower half of Table I, in which the optimal codes of lengths labeled by p are already known. For simplicity we have denoted $f_m=\frac{4^m-1}{3}\ (m\geq 1)$, i.e.,

$$\{1,5,21,85,341,\ldots,f_k=4f_{k-1}+1,\ldots\}. \tag{2}$$

All our codes either i) saturate the quantum Hamming bound (of unlabeled lengths) or ii) saturate the LP bound that has

been worked out analytically for three special families of lengths (labeled by l) or iii) have the best known parameters and are only 1 logical qubit less than the quantum Hamming bound (of lengths labeled by u).

After the introduction of some notations and known results essential to our construction in Sec.II, we shall present the general construction for the optimal code of a length $n \geq 38$ in Sec.III and then work out the LP bound for 3 families of lengths in Sec.IV to ensure the optimality of some families of our codes. In Sec. V we construct explicitly all the pure optimal codes of lengths $n \leq 37$ case by case, which are essential for our general construction.

II. Notations and known results

Our construction is based on two families pure codes and Gottesman's stabilizer pasting [7] to build new codes from old pure codes. As usual we denote by X, Y, Z three Pauli operators and by I the identity operator. Furthermore we denote $X(n) = X_1 X_2 \dots X_n$ with X_i being the Pauli operator X acting nontrivially on the i-th qubit only and similar expressions for $Y(n), Z(n)$, and $I(n)$. For simplicity we shall denote by $[n, s]$ the stabilizer of a *pure* stabilizer code $[[n, n-s, 3]]$ while simply by $[n]$ the stabilizer an *optimal* pure code of length n, e.g., [5] stands for the perfect code $[[5, 1, 3]]$ whose stabilizer reads

$$\begin{array}{|cccc|c|}\hline X & X & X & X & I \\ Z & Z & Z & Z & I \\ X & Y & Z & I & X \\ Y & Z & X & I & Z \\ \hline\end{array}, \tag{3}$$

where a juxtaposition of some Pauli operators in the same row means their direct product.

Codes family $[2^m]$ $(m \geq 3)$. The first codes family is Gottesman's family of optimal codes $[[2^m, 2^m - m - 2, 3]]$ with $m \geq 3$ that saturate the quantum Hamming bound [6]. By construction, these codes are non-degenerate and two observables $X(2^m) = X_1 \dots X_{2^m}$ and $Z(2^m) = Z_1 \dots Z_{2^m}$ are generators of the stabilizer. For simplicity we denote by $[2^m]$ a set of $m+2$ generators of the stabilizer of Gottesman's code with the first two generators being $X(2^m)$ and $Z(2^m)$.

An explicit construction of the remaining m generators are given by the check matrix $[H_m | A_m H_m]$ where $H_m = [c_0, c_1, \dots, c_{2^m-1}]$ with the $(k+1)$-th column c_k being the binary vector representing integer k $(k = 0, 1, \dots, 2^m - 1)$ and A_m is any invertible and fixed point free $m \times m$ matrix, i.e., $A_m s \neq 0$ and $A_m s \neq s$ for all $s \in F_2^m$. As an example the unique code $[2^3]$ has a stabilizer generated by

$$\begin{array}{|cccccccc|}\hline X & X & X & X & X & X & X & X \\ Z & Z & Z & Z & Z & Z & Z & Z \\ I & Z & I & Z & Y & X & Y & X \\ I & Z & X & Y & I & Z & X & Y \\ I & Y & Z & X & Z & X & I & Y \\ \hline\end{array}. \tag{4}$$

Codes family $[8 \cdot m]$ $(m \geq 3)$. The second family of codes are of parameters $[[8m, 8m - l_m - 5, 3]]$ with $l_m = \lceil \log_2 m \rceil$ that are constructed in Ref.[10]. One crucial property of this family is that they are stabilized by the all X and all Z observables $X(8m)$ and $Z(8m)$. Here we shall provide a different construction based on Gottesman's codes family.

TABLE II

Some examples from codes family $[8 \cdot m]$.

$[2^3]$	$[2^3]$	$[2^3]$
$I(2^3)$	$X(2^3)$	$Y(2^3)$
$I(2^3)$	$Y(2^3)$	$Z(2^3)$
$[8 \cdot 3] = [[24, 17, 3]]$		

$[2^3]$	$[2^3]$	$[2^3]$	$[2^3]$
$I(2^3)$	$X(2^3)$	$Y(2^3)$	$Z(2^3)$
$I(2^3)$	$Y(2^3)$	$Z(2^3)$	$X(2^3)$
$[8 \cdot 4] = [[32, 25, 3]]$			

$[2^3]$	$[2^3]$	$[2^3]$	$[2^3]$	$[2^3]$	$[2^3]$
$I(2^3)$	$Z(2^3)$	$Y(2^3)$	$X(2^3)$	$Y(2^3)$	$X(2^3)$
$X(2^3)$	$Y(2^3)$	$I(2^3)$	$Z(2^3)$	$X(2^3)$	$Y(2^3)$
$Z(2^3)$	$X(2^3)$	$Z(2^3)$	$X(2^3)$	$I(2^3)$	$Y(2^3)$
$[8 \cdot 6] = [[48, 40, 3]]$					

We divide $8m$ qubits into m blocks of 8-qubit. First 5 stabilizer of the code are $[2^3]^{\otimes m}$ whose first two generators are $X(8m)$ and $Z(8m)$. In the case of $m = 3, 4$ the codes are defined in Table II. In the case of $m \geq 5$ so that $l_m \geq 3$, the remaining l_m generators of the stabilizer are obtained from Gottesman's code $[2^{l_m}]$ by at first removing the first two generators and then removing arbitrary $2^{l_m} - m$ qubits and finally replacing each single-qubit Pauli operators X, Y, and Z in the remaining stabilizers with corresponding 8-qubit operators $X(2^3), Y(2^3)$, and $Z(2^3)$ respectively. In Table II we also present an example in the case of $m = 6$.

Obviously all $l_m + 5$ generators defined above are commuting with each other. Because of the first 5 generators of the stabilizer any 2-errors in the same 8-qubit block can be detected. For any 2 errors in two different 8-qubit blocks, the last l_m generators together with the first 2 generators defines a subcode of Gottesman's code $[2^{l_m}]$ and therefore detects all 2 errors in different blocks. Thus all 2-error can be detected so that we have constructed a pure 1-error-correcting code of length $8m$.

We shall abuse the notation slightly to denote all the codes of this family by $[8 \cdot m]$ though some of them are not optimal. In fact when $f_{r+1} + 1 \leq m \leq 2^{2r+1}$ and $\frac{2^{2r+1}+1}{3} \leq m \leq 2^{2r}$ with $r \geq 1$ the code $[8 \cdot m]$ is optimal since $l_m + 5 = s_H$ in these cases. Otherwise the code is suboptimal, i.e., $l_m + 5 = s_H + 1$.

Stabilizer pasting (Gottesman [7]): Given two non-degenerate stabilizer codes $[n_2, s_2] = \langle S_1, S_2, \dots, S_{s_2} \rangle$ and $[n_1, s_1] = \langle T_1, T_2, \dots, T_{s_1} \rangle$ of distance 3, if two observables $X(n_2)$ and $Z(n_2)$ belong to $[n_2, s_2]$, say, $S_1 = X(n_2)$ and $S_2 = Z(n_2)$, then the stabilizer defined in Table III defines a non-degenerate stabilizer code $[n_2 + n_1, s]$ with $s = \max\{s_2, s_1 + 2\}$, denoted as $[n_2, s_2] \rhd [n_1, s_1]$.

As the first example of stabilizer pasting we can obtain an optimal code $[13] = [[13, 7, 3]]$ by pasting the optimal code $[2^3]$ of length $n_2 = 8$ and $s_2 = 5$ stabilizers with the perfect code [5], i.e,, $n_1 = 5$ and $s_1 = 4$. The resulting code is of length $n_1 + n_2 = 13$ with $s_1 + 2 = 6 > s_2 = 5$ stabilizers.

If there is a third pure code $[n_3, s_3]$ with $X(n_3)$ and $Z(n_3)$ belonging to its stabilizer then the stabilizer pasting results in

TABLE III

THE STABILIZER FOR THE CODE OBTAINED FROM PASTING.

$X(n_2)$	$I(n_1)$		$X(n_2)$	$I(n_1)$
$Z(n_2)$	$I(n_1)$		$Z(n_2)$	$I(n_1)$
S_3	T_1		S_3	T_1
S_4	T_2		S_4	T_2
$\vdots$	$\vdots$	or	$\vdots$	$\vdots$
S_{s_2}	T_{s_2-2}		S_{s_1+2}	T_{s_1}
$I(n_2)$	T_{s_2-1}		S_{s_1+3}	$I(n_1)$
$\vdots$	$\vdots$		$\vdots$	$\vdots$
$I(n_2)$	T_{s_1}		S_{s_2}	$I(n_1)$

a pure code

$$[n_1+n_2+n_3, s] = [n_3, s_3] \rhd [n_2, s_2] \rhd [n_1, s_1] \quad (5)$$

with $s = \max\{s_3, s_2+2, s_1+4\}$, which can be further pasted with another code and so on. As the second example the perfect code $[[f_m, f_m-2m, 3]]$ with $f_m = \frac{4^m-1}{3}$ and $m \geq 3$ can be constructed by pasting Gottesman's codes $[2^{2l}]$ $(l = 2, 3, \ldots, m)$ with the pure perfect 5-qubit code [7], [4],

$$[f_m] = [2^{2(m-1)}] \rhd [2^{2(m-2)}] \rhd \ldots \rhd [2^4] \rhd [5]. \quad (6)$$

As the last example the optimal stabilizer code of length $8f_m$ $(m \geq 2)$ can be constructed by pasting Gottesman's codes $[2^{2l+1}]$ $(l = 1, 3, \ldots, m)$ [4]

$$[8f_m] = [2^{2m+1}] \rhd [2^{2m-1}] \rhd \ldots \rhd [2^3]. \quad (7)$$

These lengths are labeled by p in Table I.

III. GENERAL CONSTRUCTION

Our main tool is the pasting of codes to produce new codes from old ones and only pure codes can be used in the pasting. Since the optimal stabilizer code for $n = 6$ is degenerate the optimality does not ensure the pureness. Although from the upper half of Table I we know the optimal codes exist for $n \leq 37$, we have to check case by case that pure optimal codes also exist, which are essential to our construction.

Lemma 1 *Non-degenerate optimal 1-error correcting codes of lengths* $10 \leq n \leq 17$ *and* $30 \leq n \leq 37$ *exist.*

Proof: By a direct application of the stabilizer pasting to two optimal codes we obtain a previously unknown pure optimal code $[[37, 30, 3]]$ whose stabilizer reads

$$[37] = [2^5] \rhd [5]. \quad (8)$$

Also it is not difficult to check that the optimal stabilizer code $[[17, 11, 3]]$ found in Ref.[4] by a random search is non-degenerate, whose stabilizer reads

$$\begin{array}{c} IIXIZYZYXXZYIIXXY \\ IIZXIZIYYYXXZYYXX \\ IXIIXZXZYYYIYXZIY \\ IZIZZIYXYXZYZXZZX \\ XIIZYIIXZZYXYZIYX \\ ZIIXYYYIYIYXIXXZY \\ \hline [17] = [[17, 11, 3]] \end{array} \quad (9)$$

Obviously pure optimal codes of lengths 16 and 32 exist. We shall postpone the explicit constructions of the pure optimal codes of remaining lengths to Sec. V where the pasting of stabilizers is generalized to the pasting of noncommuting sets of generators. In fact all the pure optimal codes of lengths $5 \leq n \leq 37$ with $n \neq 6$ are summarized in Table IV. It is worthy of noting that there is another previously unknown optimal stabilizer code $[36] = [[36, 29, 3]]$, whose stabilizer is explicitly given in Table VI. ■

Lemma 1 ensures that there exist $[17-\beta]$ and $[37-\beta]$ for $0 \leq \beta \leq 7$, i.e, optimal pure codes of those lengths exist and have 6 and 7 generators respectively. For $n \geq 38$ we have the following general construction:

Theorem 2 *For a given length* $n \geq 38$ *if a)* $8f_m - 2 \leq n \leq f_{m+2} - 4$ *(recalling that* $f_m = \frac{4^m-1}{3}$*) for some* $m \geq 2$ *then we denote* $f_{m+2} - 4 - n = 8\alpha + \beta$ *with* $\alpha \geq 0$ *and* $0 \leq \beta \leq 7$. *The stabilizer*

$$[8 \cdot (2^{2m-1} - \alpha)] \rhd [2^{2m}] \rhd [2^{2m-2}] \rhd \ldots \rhd [2^6] \rhd [17-\beta] \quad (10)$$

defines a non-degenerate code $[[n, n-2m-4, 3]]$. *When* $m = 2$ *the stabilizer is generated by* $[8 \cdot (8-\alpha)] \rhd [17-\beta]$. *b) If* $f_{m+2} - 3 \leq n \leq 8f_{m+1} - 3$ *for some* $m \geq 2$ *then we denote* $8f_{m+1} - 3 - n = 8\alpha + \beta$ *with* $\alpha \geq 0$ *and* $0 \leq \beta \leq 7$. *The*

TABLE IV

THE STABILIZERS OF THE PURE OPTIMAL CODES $[[n, n-s, 3]]$ FOR $n \leq 37$ AND $n \neq 6$. ALL THE 2-ERROR-DETECTING BLOCKS SUCH AS $[28, 7]_2$ ARE CONSTRUCTED IN SEC. V EXPLICITLY.

n	s	Stabilizer	n	s	Stabilizer
10	6	Table VII	5	4	$[4, 4]_1 \rhd [1]_1$
11	6	$[10, 6]_1 \rhd [1]_1$	7	6	$[6, 6]_1 \rhd [1]_1$
12	6	$[10, 6]_2 \rhd [2, 4]_2$	8	5	$[2^3]$
13	6	$[10, 6]_2 \rhd [3, 4]_2$	9	6	$[6, 6]_2 \rhd [3, 4]_2$
14	6	$[10, 6]_1 \rhd [4, 4]_1$	18	7	$[10] \rhd [2^3]$
15	6	$[10] \rhd [5]$	19	7	$[18, 7]_1 \rhd [1]_1$
16	6	$[2^4]$	20	7	$[18, 7]_2 \rhd [2, 4]_2$
17	6	Eq.(9) (Ref.[4])	21	6	$[2^4] \rhd [5]$
30	7	$[28, 7]_2 \rhd [2, 4]_2$	22	7	$[18, 7]_1 \rhd [4, 4]_1$
31	7	$[28, 7]_2 \rhd [3, 4]_2$	23	7	$[18, 7]_2 \rhd [5, 5]_2$
32	7	$[2^5]$	24	7	$[8 \cdot 3]$
33	7	$[28, 7]_2 \rhd [5, 5]_2$	25	7	$[18, 7]_1 \rhd [7, 5]_1$
34	7	$[26, 7]_2 \rhd [7, 5]_1 \rhd [1]_1$	26	7	$[18, 7]_2 \rhd [7, 5]_1 \rhd [1]_1$
35	7	$[28, 7]_1 \rhd [7, 5]_1$	27	7	$[18, 7]_1 \rhd [2^3] \rhd [1]_1$
$^\alpha$36	7	$[28, 7]_2 \rhd [7, 5]_1 \rhd [1]_1$	28	7	$[20, 7]_2 \rhd [7, 5]_1 \rhd [1]_1$
$^\alpha$37	7	$[32] \rhd [5]$	29	7	$[8 \cdot 3] \rhd [5]$

stabilizer

$$[8\cdot(2^{2m}-\alpha)]\rhd[2^{2m+1}]\rhd[2^{2m-1}]\rhd\ldots\rhd[2^7]\rhd[37-\beta] \quad (11)$$

defines a non-degenerate code $[[n, n-2m-5, 3]]$. *When* $m=2$ *the stabilizer is generated by* $[8\cdot(16-\alpha)]\rhd[37-\beta]$.

Proof: At first from Lemma 1 and the constructions of two codes families $[8\cdot k]$ and $[2^k]$ it is clear that all the stabilizer codes involved in Eq.(10) or Eq.(11) are non-degenerate. Secondly by construction two families of codes $[8\cdot k]$ and $[2^k]$ are stabilized by all X and all Z Pauli operators. As a result the stabilizer pasting can be applied from right to left so that Eq.(10) and Eq.(11) define pure stabilizer codes of distance 3.

Now we evaluate the parameters of the codes. It is easy to see from the definition of α and β and identity $f_{m+2} = 2^{2m+2}+2^{2m}+\ldots+2^4+5$ that the length of the resulting codes are exactly n. Recalling that the codes $[8\cdot k]$ and $[2^k]$ have $l_k=\lceil\log k\rceil+5$ and $k+2$ stabilizers respectively while the codes $[17-\beta]$ and $[37-\beta]$ have at most 6 and 7 stabilizers respectively. Since $\alpha\geq 0$ we have $\lceil\log(2^{2m-a}-\alpha)\rceil\leq 2m-a$ for $a=0,1$, the stabilizers in Eq.(10) and Eq.(11) have $2m+4$ and $2m+5$ generators respectively. ∎

Let us look at some examples. If $n=38$ then $m=2$ so that $38\leq n\leq 81$ and the condition of case a is satisfied. In this case $81-38=5\times 8+3$ so that $\alpha=5$ and $\beta=3$ and the construction Eq.(10), i.e, $[8\cdot 3]\rhd[14]$, gives rise to a stabilizer code $[[38,30,3]]$, which is not optimal but the best code constructed so far. The situation is similar for lengths $n=39,82,83$. If $n=81$ we have

$$[81]=[2^6]\rhd[17], \quad (12)$$

an optimal code $[[81,73,3]]$ obviously missing from the public code table. If $n=371$ then $m=3$ and $340\leq n\leq 677$ with the condition of case b satisfied. In this case $677-371=8\times 38+2$ so that $\alpha=38$ and $\beta=2$ and by construction Eq.(11) we have $[371]=[8\cdot 26]\rhd[2^7]\rhd[35]$ which is an optimal code $[[371,360,3]]$ that saturates the quantum Hamming bound.

Remarks For any given $n\geq 38$ we have either construction a or construction b. Generally:

i) In the case of $8f_m+3\leq n\leq f_{m+2}-4$ or $f_{m+2}+1\leq n\leq 8f_{m+1}-3$ (unlabeled lengths in Table I) we have $m=\lfloor\frac{s_H-4}{2}\rfloor$ and Theorem 2 gives rise to an optimal code because the quantum Hamming bound is saturated, i.e., its stabilizer has s_H generators.

ii) In the case of $n=8f_m$ or $n=f_{m+2}$ with $m\geq 2$ (lengths labeled by p in Table I) the construction of Theorem 2 gives rise to a suboptimal code that is one logical qubit less than the optimal code given in Eq.(6) or Eq.(7).

iii) In the case of $n=8f_m-\{1,2\}$ or $n=f_{m+2}-\{2,3\}$ with $m\geq 2$ (lengths labeled by u in Table I) Theorem 2 gives rise to a so-far optimal code because in these cases its stabilizer has s_H+1 generators and there is no better code known so far. However there may exist better codes with one more logical qubit.

iv) In the case of $n=8f_m+\{1,2\}$ or $n=f_{m+2}-1$ with $m\geq 2$ (lengths labeled by l in Table I) Theorem 2 gives rise also to a code with s_H+1 stabilizers, i.e., one logical qubit less than that specified by the quantum Hamming bound. However it can be proved via linear programming bound that the codes constructed via Theorem 2 are optimal in these cases. □

IV. The linear programming bound

In this section we shall work out analytically the LP bound for three families of lengths. For a stabilizer code $[[n,k,d]]$ we denote P as its projector and $K=2^k$ and $s=n-k$. The weight distributions A_i [14], [11] are defined by

$$A_i=\frac{1}{K^2}\sum_{|\omega|=i}|\mathrm{Tr}(PE_\omega)|^2 \quad (i=0,1,\ldots,n). \quad (13)$$

where the summation is over all errors supported on i qubits. It is obvious that $A_i\geq 0$, $A_0=1$, and $\sum_i A_i=2^s$ so that $\{A_i/2^s\}_{i=1}^n$ can be regarded as a probability distribution. For an arbitrary function $f(x)$ we denote its average by

$$\langle f(x)\rangle\equiv\frac{1}{2^s}\sum_{i=0}^{d}f(i)A_i. \quad (14)$$

In the following we shall formulate a subset of the linear programming bound for 1-error correcting code, which serve our purpose perfectly. For a complete set of linear programming bound see Ref.[4], [12].

Linear Programming bound (Restricted set) If there exists a stabilizer code $[[n,k,3]]$ then the following conditions hold true

$$A_1=\langle 3n-4x\rangle, \quad (15)$$

$$A_2=\frac{1}{2}\langle(4x-3n+1)^2-3n-1\rangle, \quad (16)$$

$$\sum_{i=0}^{\lfloor\frac{n}{2}\rfloor}A_{2i}\geq 2^{s-1}. \quad (17)$$

Conditions Eq.(15) and Eq.(16) come from the error-correction conditions and condition Eq.(17) comes from the fact that the even-supported subset of a stabilizer is a half or the whole stabilizer.

Theorem 3 *If there exists a stabilizer code* $[[n,k,3]]$, *degenerate or non-degenerate, for a length* n *equals* $f_{m+2}-1$ *or* $8f_m+1$ *or* $8f_m+2$ *with* $f_m=\frac{4^m-1}{3}$ *and* $m=1,2,\ldots$, *then* $n-k\geq s_H+1$, *while the quantum Hamming bound for the 1-error-correcting stabilizer codes of length* n *reads* $n-k\geq s_H=\lceil\log_2(3n+1)\rceil$.

Proof: Suppose that $n=f_{m+2}-1$ with $m\geq 1$ it is obvious that $\frac{3n}{4}=4^{m+1}-1$ is an integer and therefore the following function

$$h(x)=16\left(x-\frac{3n}{4}\right)\left(x-1-\frac{3n}{4}\right) \quad (18)$$

is nonnegative for all integers. Specifically $h(x)\geq 0$ for $x=0,1,2,\ldots,n$. Furthermore we have

$$h(0) = 3n(3n+4), \quad (19)$$

$$h(1) = 3n(3n-4)>2(3n+4)\ (n\geq 3), \quad (20)$$

$$h(2) = (3n-4)(3n-8)\geq 2(3n+4)\ (n\geq 3). \quad (21)$$

In this case the quantum Hamming bound reads $s_H = 2m+4$ (since $3n+4 = 2^{2m+4}$) and we shall prove $n-k \geq s_H+1$ if there exists a stabilizer code $[[n,k,3]]$, which means Eqs.(15-17) must hold. As a result we have

$$\langle h(x)\rangle = 3n + 2A_1 + 2A_2. \quad (22)$$

Thus it follows from

$$\begin{aligned} 2^s\langle h(x)\rangle &= \sum_{i=0}^{n} h(i)A_i \geq h(0) + h(1)A_1 + h(2)A_2 \\ &\geq (3n+4)(3n+2A_1+2A_2) \\ &= (3n+4)\langle h(x)\rangle \end{aligned} \quad (23)$$

that $2^s \geq 3n+4$, i.e., $n-k \geq s_H$. We shall now prove that the equality can never happen. If the equality were true, i.e., $2^s = 3n+4$, then all the inequalities in Eq.(23) would become equalities which means that $A_i = 0$ except $i = 0, l, l+1$ where $l = 3n/4$ since $l, l+1$ are the only zeros of $h(x)$. From conditions $1 + A_l + A_{l+1} = 3n+4$ and $3n - 4A_{l+1} = 0$, which comes from Eq.(15), we can solve $A_{l+1} = 3n/4$ and $A_l = 9n/4 + 3$. Noticing that $l = 4^{m+1} - 1$ is odd it follows from inequality Eq.(17) that $1 + 3n/4 \geq (3n+4)/2$ which is impossible. Thus $2^s > 3n+4$, i.e, $n-k \geq s_H + 1$.

The cases $n = 8f_m + \{1, 2\}$ have been proved in [17] here we shall reproduce them for completeness. At first we suppose $n = 8f_m + 1$ with $m \geq 1$. In this case $s_H = 2m+3$ and we introduce a nonnegative function as

$$f(x) = 16\left(x - \frac{3n+1}{4}\right)^2. \quad (24)$$

It is easy to check that as long as $n \geq 5$

$$f(0) = (3n+1)^2 > (3n+5)(3n-7) + 16, \quad (25)$$
$$f(1) = (3n-3)^2 > 4(3n+5), \quad (26)$$
$$f(2) = (3n-7)^2 > 2(3n+5) + 16. \quad (27)$$

If there exists a stabilizer code $[[n,k,3]]$ then Eqs.(15-17) must hold. As a result of Eqs.(15-16) we have

$$\langle f(x)\rangle = 3n + 1 + 4A_1 + 2A_2. \quad (28)$$

As a result of Eq.(17) we have

$$16A_0 + 16A_2 + \sum_{i=2}^{4f_m} f(2i)A_{2i} \geq 16\sum_{i=0}^{4f_m} A_{2i} \geq 8.2^s, \quad (29)$$

where we have used $f(2i) \geq 16$ since $\frac{3n+1}{4}$, the unique zero of $f(x)$, is an odd integer. Putting all these pieces together

$$\begin{aligned} 2^s\langle f(x)\rangle &= \sum_{i=0}^{n} f(i)A_i \\ &\geq f(0) + f(1)A_1 + f(2)A_2 + \sum_{i=2}^{4f_m} f(2i)A_{2i} \\ &\geq f(0) - 16 + f(1)A_1 + (f(2)-16)A_2 + 8.2^s \\ &> (3n+5)(3n-7+4A_1+2A_2) + 8.2^s \\ &= (3n+5)\langle f(x) - 8\rangle + 8.2^s, \end{aligned} \quad (30)$$

in which the strict inequality comes from the $f(0)$ term. As a result we have $2^s > 3n+5 = 2^{s_H}$, taking into account of $\langle f(x)\rangle > 8$. That is equivalent to saying $n-k \geq s_H + 1$.

Now we suppose $n = 8f_m + 2$ with $m \geq 1$ and in this case $s_H = 2m+3$. Since $\frac{3n+2}{4}$ is an integer the function defined as follows

$$g(x) = 16\left(x - \frac{3n+2}{4}\right)\left(x - \frac{3n-2}{4}\right) \quad (31)$$

is nonnegative for integer x. It is obvious that $g(0) > (3n+2)(3n-4)$ and $g(i) > 2(3n+2)$ for $i = 1, 2$ as long as $n \geq 5$. If there exists a stabilizer code $[[n,k,3]]$ then Eqs.(15-17) must hold, which leads to

$$\langle g(x)\rangle = 3n - 4 + 2A_1 + 2A_2. \quad (32)$$

Thus

$$\begin{aligned} 2^s\langle g(x)\rangle &\geq g(0) + g(1)A_1 + g(2)A_2 \\ &> (3n+2)(3n-4+2A_1+2A_2) \\ &= (3n+2)\langle g(x)\rangle. \end{aligned} \quad (33)$$

The strict inequality sign is due to the $g(0)$ term. Since $\langle g(x)\rangle > 0$ we have $2^s > 3n+2 = 2^{s_H}$, i.e., $n-k \geq s_H + 1$. ■

V. Special constructions

In this section we shall prove Lemma 1 by constructing explicitly all the optimal non-degenerate codes with lengths $n \leq 37$ except $n = 6$. Our main tool is a generalization of the pasting of stabilizer codes to a pasting of 2-error detecting blocks (2ed-block) defined as below.

Definition 4 *A 2-error detecting block $[n,s]_e$ is generated by a set of s multilocal Pauli operators acting on n qubits with e pairs being non-commuting that detects up to 2-qubit errors.*

Each non-degenerate stabilizer code $[n,s]$ detect all 2-error and so they define 2ed-blocks $[n,s]_0$ with all the generators being commuting. By shortening a pure code we generally obtain 2ed-blocks with some noncommuting pairs of generators. Some examples of 2ed-blocks are presented in Table V.

2ed-blocks pasting: Given two 2ed-blocks $[n_2,s_2]_{e_2}$ and $[n_1,s_1]_{e_1}$ that are generated by $\langle S_1 = X(n_2), S_2 = Z(n_2), \ldots, S_{s_2}\rangle$ and $\langle T_1, T_2 \ldots, T_{s_1}\rangle$ respectively, then $s = \max\{s_1, s_2+2\}$ generators as given in Table III is a 2-ed block $[n_1+n_2, s]_e$ with $|e_1 - e_2| \leq e \leq e_1 + e_2$. For convenience we shall denote by $[n_1,s_2]_{e_1} \rhd [n_2,s_1]_{e_2}$ the resulting 2ed-block.

TABLE V
SOME EXAMPLES OF 2-ERROR-DETECTING BLOCKS.

$X\ I$	$X\ X\ X$	$X\ X\ X\ X$
$Z\ I$	$Z\ Z\ Z$	$Z\ Z\ Z\ Z$
$I\ X$	$X\ Y\ Z$	$X\ Y\ Z\ I$
$I\ Z$	$Y\ Z\ X$	$Y\ Z\ X\ I$
$[2,4]_2$	$[3,4]_2$	$[4,4]_1$

$X\ X\ X$	$X\ X\ X\ X\ X$	$X\ X\ X\ X\ X\ X\ X$
$Z\ Z\ Z$	$Z\ Z\ Z\ Z\ Z$	$Z\ Z\ Z\ Z\ Z\ Z\ Z$
$Z\ I\ Z$	$Y\ X\ Y\ X\ I$	$Z\ I\ Z\ Y\ X\ Y\ X$
$Z\ X\ Y$	$I\ Z\ X\ Y\ I$	$Z\ X\ Y\ I\ Z\ X\ Y$
$Y\ Z\ X$	$Z\ X\ I\ Y\ I$	$Y\ Z\ X\ Z\ X\ I\ Y$
$[3,5]_2$	$[5,5]_2$	$[7,5]_1$

The 2ed-block given in Table III detects up to 2-qubits errors because firstly all the errors happening on the n_1-block or n_2-block can be detected because $[n_1, s_1]_{e_1}$ and $[n_2, s_2]$ are two pure codes of distance 3 and secondly two qubits errors happening on different blocks can be detected by the first two generators $X(n_2) \otimes I(n_1)$ and $Z(n_2) \otimes I(n_1)$. If two noncomuting generators are arranged in the same row the resulting generators will become commuting. As a result e can be zero when $e_1 = e_2$ and all noncommuting pairs are carefully matched. In this case we obtain a pure 1-error-correcting stabilizer code, since all 2-qubit errors can be detected.

From the above arguments we see that although the 1-qubit block, denoted as $[1]_1 = \langle X, Z\rangle$, detects only single qubit errors, it can be regarded as a 2ed-block because there is no 2-qubit errors on a single qubit block. For example we have $[2, 4]_2 = [1]_1 \rhd [1]_1$. As another example the perfect code $[[5, 1, 3]]$ in Eq.(3) can be regarded as the pasting of two 2ed-blocks $[4, 4]_1 \rhd [1]_1$.

A 2ed-block fails to define a code because there are some pairs of noncommuting generators. By pasting two or more 2ed-blocks these noncommuting generators may become commuting and we thus obtain a 1-error correcting stabilizer code. Our construction is therefore a kind of puncturing plus pasting. By puncturing some old stabilizer codes we obtain some 2ed-blocks that generally contains some pairs of noncommuting generators. By pasting with some other 2ed-blocks and carefully matching their noncommuting pairs we are able to produce some new stabilizer codes. To complete the constructions given in Table IV we have only to construct explicitly all the relevant 2ed-blocks.

We consider the optimal code $[2^5]$ as in Table VI whose stabilizer is defined by the check matrix $[RH_5|A_5RH_5]$ with

$$A_5 = \begin{pmatrix} 1\,1\,0\,0\,0 \\ 1\,1\,0\,1\,0 \\ 0\,1\,0\,0\,0 \\ 0\,1\,1\,0\,1 \\ 0\,1\,1\,0\,0 \end{pmatrix}, \quad R = \begin{pmatrix} 1\,0\,0\,0\,0 \\ 0\,0\,0\,0\,1 \\ 0\,1\,0\,0\,0 \\ 0\,0\,0\,1\,0 \\ 1\,1\,1\,0\,0 \end{pmatrix}. \qquad (34)$$

Obviously A_5 is revertible and fixed-point free and R is invertible. By removing four coordinates $[c_5, c_{10}, c_{19}, c_{28}]$ from this $[2^5]$ we obtain the 2ed-block $[28, 7]_2$ and by removing the first four coordinates $[c_0, c_1, c_2, c_3]$ we obtain A 2ed-block $[28, 7]_1$. By 2ed-blocks pasting with 2ed-blocks in Table V we obtain the pure optimal codes of lengths $30, 31, 33$ and 35 in addition to a previously unknown optimal code

$$[36] = [28, 7]_2 \rhd [7, 5]_1 \rhd [1]_1 \qquad (35)$$

whose stabilizer is explicitly given in Table VI.

From three partitions of $[2^4]$ as shown in Table VII we can obtain a pure optimal code $[10]$ as well as the unique optimal code $[[6, 0, 4]]$ of distance 4 and four different 2ed-blocks. By pasting with the perfect 5-qubit code we obtain $[15] = [10] \rhd [5]$. Also we obtain all the optimal pure codes of lengths from 11 to 14 as well as an optimal pure $[7] = [6, 6]_1 \rhd [1]_1$. Finally the remaining 2ed-blocks appeared in Table IV are given in Table VIII.

TABLE VII

THREE PARTITIONS OF THE OPTIMAL CODE $[2^4]$.

$[2^4] = [[16, 10, 3]]$

$X\,X\,X\,X\,X\,X\,X\,X\,X\,X$	$X\,X\,X\,X\,X\,X$
$Z\,Z\,Z\,Z\,Z\,Z\,Z\,Z\,Z\,Z$	$Z\,Z\,Z\,Z\,Z\,Z$
$I\,X\,Y\,Z\,I\,I\,I\,X\,Y\,Z$	$Y\,X\,Z\,Z\,Y\,X$
$I\,Y\,Z\,X\,I\,I\,I\,Y\,Z\,X$	$Z\,Y\,X\,X\,Z\,Y$
$I\,I\,I\,I\,X\,Y\,Z\,X\,Z\,Y$	$X\,Y\,Z\,X\,Y\,Z$
$I\,I\,I\,I\,Y\,Z\,X\,Y\,X\,Z$	$Y\,Z\,X\,Y\,Z\,X$
$[10] = [[10, 4, 3]]$	$[[6, 0, 4]]$

$X\,X\,X\,X\,X\,X\,X\,X\,X\,X$	$X\,X\,X\,X\,X\,X$
$Z\,Z\,Z\,Z\,Z\,Z\,Z\,Z\,Z\,Z$	$Z\,Z\,Z\,Z\,Z\,Z$
$I\,X\,Y\,Z\,Y\,X\,Z\,Z\,Y\,X$	$I\,I\,I\,X\,Y\,Z$
$I\,Y\,Z\,X\,Z\,Y\,X\,X\,Z\,Y$	$I\,I\,I\,Y\,Z\,X$
$I\,I\,I\,I\,X\,Y\,Z\,X\,Y\,Z$	$X\,Y\,Z\,X\,Z\,Y$
$I\,I\,I\,I\,Y\,Z\,X\,Y\,Z\,X$	$Y\,Z\,X\,Y\,X\,Z$
$[10, 6]_1$	$[6, 6]_1$

$X\,X\,X\,X\,X\,X\,X\,X\,X\,X$	$X\,X\,X\,X\,X\,X$
$Z\,Z\,Z\,Z\,Z\,Z\,Z\,Z\,Z\,Z$	$Z\,Z\,Z\,Z\,Z\,Z$
$I\,X\,Y\,Z\,I\,I\,I\,X\,Y\,Z$	$Y\,Z\,X\,Z\,X\,Y$
$I\,Y\,Z\,X\,I\,I\,I\,Y\,Z\,X$	$Z\,X\,Y\,X\,Y\,Z$
$I\,I\,I\,I\,X\,Y\,Z\,X\,Y\,Z$	$X\,Y\,Z\,X\,Y\,Z$
$I\,I\,I\,I\,Y\,Z\,X\,Y\,Z\,X$	$Y\,Z\,X\,Y\,Z\,X$
$[10, 6]_2$	$[6, 6]_2$

TABLE VIII

FURTHER CONSTRUCTIONS OF 2ED-BLOCKS.

$[5,5]_2$	$[5,5]_2$	$[5,5]_2$	$[3,5]_2$
$I(5)$	$X(5)$	$Y(5)$	$Z(3)$
$I(5)$	$Y(5)$	$Z(5)$	$X(3)$
$[18, 7]_1$			

$[7,5]_1$	$[5,5]_2$	$[3,5]_2$	$[3,5]_2$
$I(7)$	$X(5)$	$Y(3)$	$Z(3)$
$I(7)$	$Y(5)$	$Z(3)$	$X(3)$
$[18, 7]_2$			

$[7,5]_2$	$[5,5]_2$	$[5,5]_2$	$[3,5]_2$
$I(7)$	$X(5)$	$Y(5)$	$Z(3)$
$I(7)$	$Y(5)$	$Z(5)$	$X(3)$
$[20, 7]_2$			

$[7,5]_2$	$[7,5]_2$	$[7,5]_2$	$[5,5]_2$
$I(7)$	$X(7)$	$Y(7)$	$Z(5)$
$I(7)$	$Y(7)$	$Z(7)$	$X(5)$
$[26, 7]_2$			

VI. DISCUSSIONS

We prescribe a general construction of all the optimal stabilizer codes of distance 3 for lengths $n \geq 38$ by pasting known codes and a special construction of the optimal pur stabilizer codes of length $5 \leq n \leq 37$ case by case by employing a generalization of the stabilizer pasting to noncommuting set of stabilizers, i.e., 2ed-blocks pasting. For three families of lengths we have worked out analytically the linear programming bound, which is strictly stronger than the quantum Hamming bound and ensures the optimality of our codes for these lengths. Except $n = 6$ all the optimal codes are pure.

Apparently the construction given by Theorem 2 is not unique. Firstly there are different constructions for the optimal

TABLE VI

THE STABILIZER FOR THE OPTIMAL CODE $[[36, 29, 3]]$.

$[[32, 25, 3]]$

5	10	19	28	0	1	2	3	4	6	7	8	9	11	12	13	14	15	16	17	18	20	21	22	23	24	25	26	27	29	30	31								
X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	I	I	I	I	I	I	I	I
Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	I	I	I	I	I	I	I	I
Z	I	X	Y	I	Z	I	Z	I	I	Z	I	Z	Z	I	Z	I	Z	Y	X	Y	Y	X	Y	X	Y	X	Y	X	X	Y	X	X	X	X	X	X	X	X	X	I
Y	Z	Y	Z	I	Y	Z	X	I	Z	X	I	Y	X	I	Y	Z	X	Z	X	I	Z	X	I	Y	Z	X	I	Y	X	I	Y	Z	Z	Z	Z	Z	Z	Z	Z	I
Z	X	Z	X	I	Z	I	Z	I	I	Z	X	Y	Y	X	Y	X	Y	I	Z	I	I	Z	I	Z	X	Y	X	Y	Y	X	Y	Y	Z	X	Z	X	I	Y	X
I	X	X	I	I	Z	X	Y	Z	Y	X	I	Z	Y	Z	I	Y	X	Z	I	Y	I	Z	X	Y	Z	I	Y	X	Z	X	Y	Z	X	Y	I	Z	X	Y	Z
Y	Y	Y	Y	I	Z	I	Z	X	X	Y	Y	X	X	Z	I	Z	I	X	Y	X	I	Z	I	Z	Z	I	Z	I	X	Y	X	Z	I	Z	Y	X	Y	X	I
				$[28, 7]_2$																												$[7, 5]_1$							$[1]_1$

code $[2^m]$ [4]. Secondly there are other constructions such as

$$[8 \cdot (2^{2m-1} - \alpha_1)] \rhd [8 \cdot (2^{2m-3} - \alpha_2)] \rhd \ldots \\ \ldots \rhd [8 \cdot (2^3 - \alpha_{m-1})] \rhd [17 - \beta] \qquad (36)$$

or

$$[8 \cdot (2^{2m} - \alpha_1)] \rhd [8 \cdot (2^{2m-2} - \alpha_2)] \rhd \ldots \\ \ldots \rhd [8 \cdot (2^4 - \alpha_{m-1})] \rhd [37 - \beta] \qquad (37)$$

where $\alpha_i + 3 \leq 2^{2(m-i+1)-1}$ or $2^{2(m-i+1)}$ respectively and $\alpha = \sum_{i=1}^{m-1} \alpha_i$. For different choices of $\{\alpha_i\}$ the resulting codes may be inequivalent. One problem arises as to the classification of all the optimal codes. Finally our approach can be easily adapted to nonbinary codes.

REFERENCES

[1] A. Ashikhmin and S. Litsyn, "Upper bounds on the size of quantum codes", IEEE Trans. Inform. Theory, vol. 45, no. 4, pp. 1206-1215, 1999.

[2] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, andW. K.Wootters, Phys. Rev. A 54, 3824 (1996).

[3] A. Calderbank, E. Rains, P. Shor, and N. Sloane, "Quantum error correction and orthogonal geometry", Phys. Rev. Lett., vol. 76, pp. 405-409, 1997.

[4] ———, "Quantum error correction via codes over GF(4)", IEEE Trans. Inform. Theory, vol. 44, pp. 1369-1387, 1998.

[5] D. Gottesman, "Stabilizer codes and quantum error correction", 1997, Caltech Ph. D. Thesis, eprint: quant-ph/9705052.

[6] ———, "A class of quantum error-correcting codes saturating the quantum Hamming bound", Phys. Rev. A, vol. 54, pp. 1862-1868, 1996.

[7] ———, "Pasting quantum codes", 1996, eprint: quant-ph/9607027.

[8] M. Grassl, "Bounds on the minimum distance of linear codes." Online available at http://www.codetables.de. Accessed on 2009-01-02.

[9] E. Knill and R. Laflamme, "A theory of quantum errorcorrecting codes", Phys. Rev. A 55, no. 2, pp. 900-911, 1997.

[10] R. Li and X. Li, "Binary construction of quantum codes of minimum distance three and four", IEEE Trans. Inf. Theory, vol. 50, no. 6, pp. 1331-1336, 2004.

[11] E. Rains, "Quantum weight enumerators", IEEE Trans. Inform. Theory, vol. 44, no. 4, pp. 1388-1394, 1998.

[12] ———, "Quantum shadow enumerators", IEEE Trans. Inform. Theory, vol. 45, no. 7, pp. 23612366, 1999.

[13] P. W. Shor, "Scheme for reducing decoherence in quantum memory", Phys. Rev. A, vol. 2, pp. 2493-2496, 1995.

[14] P. Shor and R. Laflamme, "Quantum analog of the MacWilliams identities in classical coding theory", Phys. Rev. Lett., vol. 78, pp. 1600-1603, 1997.

[15] A. Steane, "Error Correcting Codes in Quantum Theory", Phys. Rev. Lett., vol. 77, no. 5, pp. 793-797, July 1996.

[16] ———, "Enlargement of Calderbank-Shor-Steane quantum codes", IEEE Trans. inf. 45, Issue 7, Nov 1999 Page(s): 2492 - 2495.

[17] S. Yu, Q. Chen, and C.H. Oh, "Two infinite families of nonadditive quantum error-correcting codes", arXiv: 0901.1935 [quant-ph].